STADIA
HELSINGIN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN TOIMIALA

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

LANGATTOMAT ETHERNET-TEKNOLOGIAT JA NIIDEN VERKKOTURVA

Työn tekijä: Tomi Niemi

Työn valvoja: Jukka Louhelainen

Työn ohjaaja: Petteri Hallikainen

Työ hyväksytty: __. __. 2007

Jukka Louhelainen

lehtori

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ALKULAUSE

Tämä insinöörityö tehtiin Oy TietoEnator Ab:n antamasta aiheesta osana Helsingin ammattikorkeakoulun insinöörikoulutusta. Insinöörityön tekeminen osoittautui kaikista koulutukseen kuuluvista osista haasteellisimmaksi.

Työn varsinainen sisältö oli alusta alkaen selvä, kiitos tästä Petteri Hallikaiselle, joka osasi kertoa tarkasti mitä työhön halusi. Työn varsinainen aloittaminen ja sen loppuun saattaminen vaativat veronsa, niin fyysisesti kuin henkisestikin.

Tämä työ on kuusivuotisen urakan viimeinen vaihe ennen valmistumistani. Haluaisin kiittää ystäviäni ja perhettäni saamastani tuesta opiskelujeni aikana sekä opinnäytetyön tekemiseen painostamisesta, ilman heitä ei työ olisi todennäköisesti ikinä valmistunut.

Helsingissä 12.4.2007

Tomi Niemi

STADIA
HELSINGIN AMMATTIKORKEAKOULU

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Tomi Niemi	
Työn nimi: Langattomat Ethernet-teknologiat ja niiden verkkoturva	
Päivämäärä: 13.4.2007	Sivumäärä: 42
Koulutusohjelma: Tietotekniikka	Suuntautumisvaihtoehto: Tietoliikennetekniikka
Työn valvoja: lehtori Jukka Louhelainen Työn ohjaaja: Petteri Hallikainen	

Tässä opinnäytetyössä tutustutaan IEEE 802.11 -standardien perheeseen. Työssä esitellään WLAN-yhteyksien evoluutio nykypäivään asti ja niiden suojaus. Lisäksi esitellään kaksi muuta langattoman yhteyden standardia, IEEE 802.16 ja IEEE 802.16, jotka on suunniteltu kattamaan kaupunkialueita.

Työ on tehty täysin kirjallisuustutkielmana. Lähteinä on käytetty sekä painettua kirjallisuutta että Internet-lähteitä.

WLAN-yhteys tuo mukanaan lähes kaapelittoman verkon, mutta samalla se tarjoaa mahdollisuuden hyväksikäyttää yhteyttä. Tukiasemat ovat oletuksena suojaamattomia ja harva kotikäyttäjä ymmärtää edes mitä langattoman verkon suojaaminen tarkoittaa.

Yrityksissä WLAN-suojaus tulisi ottaa edellistä vakavammin, yrityksen liikesalaisuuksien vuotaminen WLAN-yhteyden kautta tulisi olla mahdotonta.

Pääpaino työssä on suojaustapojen käsittelyssä mahdollisimman laajasti. Lisäksi annetaan ehdotus kuinka suojata langaton lähiverkko niin kotona kuin yrityksessä.

Työtä voidaan käyttää apuna suunnitellessa WLAN-verkon suojaamista.

Avainsanat: 802.11, 802.16, 802.20, Langaton, RADIUS, Suojaus, WEP, WLAN, WPA.

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ABSTRACT

Name:
Tomi Niemi

Title:
Wireless Ethernet technologies and Wireless Security

Date:
13.4.2007

Number of pages:
42

Department:
Communications

Study Programme:
Telecommunications

Instructor:
Jukka Louhelainen

Supervisor:
Petteri Hallikainen

This study focuses on the IEEE 802.11 standards family. The evolution of WLAN connections from the first released standard to present day is covered. Additionally two other wireless connection standards are introduced, the IEEE 802.16 and IEEE 802.20, which are designed mainly for metropolitan areas.

This thesis has been carried out as a desk research. Internet and relevant literature were used as sources of information. Due to the fast development of the wireless world, more internet sources were used.

WLAN offers a great deal of ease. The possibility of virtually no cables has increased the number of wireless clients, but at the same time people tend to forget about security. Most of the access points sold today are by default without any protection and only few users even understand the importance of secured networks. In corporate networks it should be impossible to leak information through wireless connections.

The main emphasis of this study is to cover the available security schemes as broadly as possible. This study will conclude in a suggestion to build a secure network for both home and corporate networks.

This study can be used to help determine the appropriate protection when building a wireless network.

Keywords: 802.11, 802.16, 802.20, RADIUS, Security, Wireless, WEP, WLAN, WPA.

SISÄLLYS

1 JOHDANTO

Langattomat verkot ovat yleistyneet sitä mukaa, mitä halvemmaksi laitteet ja laajakaistayhteydet ovat tulleet. Tässä työssä käsitellään langattomien lähiverkkojen standardit ja perehdytään niiden ominaisuuksiin. Lisäksi käsitellään kaksi muuta langattoman yhteyden standardia; 802.16 eli WiMAX sekä 802.20 eli mobiili langaton yhteys. Tärkeimpänä aiheena työssä on kuitenkin langattomien verkkojen suojaus sekä koti- ja yritysverkoissa ja kuinka se toteutetaan.

Ensimmäisenä tutustutaan IEE802.11 protokollapinoon ja siihen miten paketti rakentuu kun se kulkee pinon läpi. Kolmannessa kappaleessa tutustutaan IEEE 802.11a/b/g -standardien rakenteeseen ja niiden ominaisuuksiin jotta lukijalle tulisi jonkinlainen käsitys mistä osista yhteys periaatteessa muodostuu. Neljännessä ja viidennessä kappaleessa käydään pikaisesti läpi, lähinnä pintapuolin, kaksi muuta langatonta standardia; IEEE 802.16 ja IEEE 802.20.

Standardien jälkeen siirrytään työn varsinaiseen aiheeseen, langattomien lähiverkkojen suojaukseen. Kuudes kappale käsittelee yleisimmät suojaustavat, jotka ovat helposti kuluttajienkin käytettävissä. Samassa kappaleessa perehdytään myös lähinnä yrityksille ja isommille verkoille tarkoitettuihin suojaustapoihin. Nämä vaativat ulkoisen palvelimen, kuten RADIUS, ja verkon ylläpitoa asiantuntijan toimesta.

Työn viimeisessä kappaleessa edellä esitellyistä suojaustavoista arvioidaan paras ja tehokkain suojaus. Lisäksi annetaan ehdotus kuinka rakentaa langaton lähiverkko niin kotiin kuin yritykseen.

Työ vastaa kysymyksiin kuten; miten langaton lähiverkko rakennetaan, miten se suojataan ja kuinka voidaan varmistaa että yrityksen verkkoon ei murtauduta?

2 IEEE 802.11

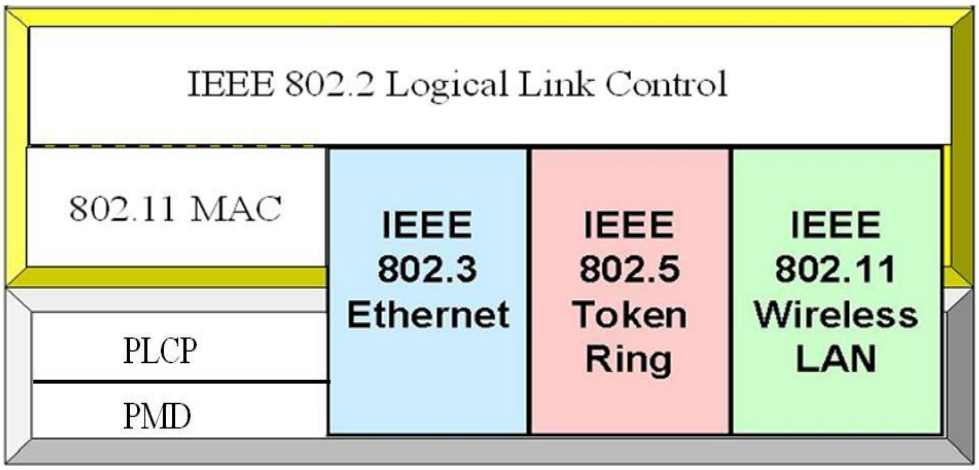
IEEE 802.11 -työryhmä on osa IEEE 802 LAN/MAN standardointikomiteaa, joka toimii maailman laajimman professionaalisen organisaation, IEEE:n (Institute of Electrical and Electronic Engineers) suojissa. Komitean osanottajat, jotka vastaavat standardien käyttöönotosta ja kehittämisestä, koostuvat laitevalmistajista, operaattoreista, akateemikoista ja konsultanteista ympäri maailman. WLAN-yhteydestä käytetään nimitystä Wi-Fi, joka on Wi-Fi Alliancen tavaramerkki. WiFi-allianssi on WLAN-valmistajien yhteinen sertifiointi- ja markkinointiorganisaatio, jonka sertifioimat laitteet toimivat muiden sertifioitujen laitteiden kanssa.

IEEE julkaisi ensimmäisen standardin langattomille lähiverkoille vuonna 1997. Se sai nimekseen IEEE 802.11. Standardi osoittautui nopeasti kuitenkin jo liian hitaaksi monille sovelluksille. Nopeus oli vain 2 Mbps, joka jäi selvästi alle muutamia vuosia aikaisemmin julkaistun Fast Ethernet –lähiverkon nopeuksien. Lisäksi yhteensopivuusongelmat ja taajuuskaistaan liittyvät käyttölupaongelmat saivat aikaan sen, että standardin pohjalta alettiin kehittää uusia standardeja. [1.]

2.1 Fyysinen kerros ja Siirtoyhteyskerros

IEEE 802 -standardit kattavat OSI (Open System Interconnection) –mallin kaksi alinta kerrosta: fyysisen kerroksen (Physical Layer) ja siirtoyhteyskerroksen (Data Link Layer). [2.]

Siirtoyhteyskerros (Layer 2) on jaettu kahteen osaan: siirtotien ohjaukseen (Logical Link Control, LLC) ja vuoronvaraukseen (Medium Access Control, MAC). 802.2 LLC muodostaa yhteisen rajapinnan kaikille 802.x-verkoille. Toisin kuin perinteisissä 802.x -lähiverkoissa, langattomissa 802.11-verkoissa käytetään LLC-protokollaa ja -kehystystä. Seuraavana käydään läpi 802.11-verkkojen protokollapino ylhäältä alaspäin, kuten kuvassa 1 on esitetty.

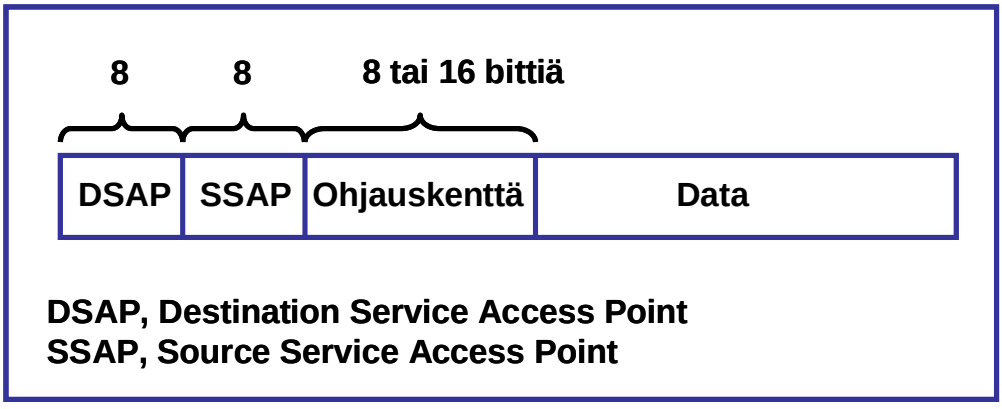


Kuva 1. 802.11-standardin protokollapino

2.2 802.2 Logical Link Control ja Sub Network Access Protocol

802.2 LLC on identtinen kaikille verkkotopologioille. Se tarjoaa yleisen rajapinnan verkkokerroksen eri protokollien (TCP/IP, IPX, yms.) ja eri verkkotyyppien (Ethernet, Token Ring, yms.) välille.

802.2 LLC tarjoaa palveluja verkkokerrokselle. Yleisimmin käytössä on kuittaamaton yhteydetön datapalvelu, jossa verkkokerroksen IP-paketti kehystetään LLC-kehykseen (kuva 2). Kehyksen otsikko sisältää protokollatunnukset ja ohjauskentän.



Kuva 2. LLC-kehys

Vaikka IP-protokollalle on käytössä LLC-protokollatunnus SAP (Service Access Point), käytetään yleensä SNAP-kehystystä (Sub Network Access Protocol).

SNAP-kehystystä käyttämällä voidaan IP-protokolla tunnistaa Ethernet-kehyksen mukaisella EtherType-tunnuksella. SNAP tukee myös valmistaja-kohtaisia protokollatunnisteita. Niitä käytetään myös muiden kuin IEEE 802 fyysistä kerrosta käyttävien standardien kanssa, kuten valokuitua käyttävä FDDI, Fiber-Distributed Data Interface, joka kuitenkin käyttää 802.2 LLC:tä.

SNAP-kehys on LLC-kehyksen otsikon jatkeena, otsikossa olevat SAP-protokollatunnukset ilmoittavat hexadesimaaliarvolla AA tai AB, onko kyseessä SNAP-paketti. SNAP-kehys on 5-oktettinen protokollan tunnistusosio, joka koostuu 3 oktettisesta IEEE:n määrittämästä OUI:sta (Organizationally Unique Identifier) ja 2 oktettisesta protokollatunnisteesta, protocol ID:stä.

OUI kertoo protokollan laitetoimittajan, -valmistajan tai muun organisaation. Jos OUI:n arvo on hexadesimaaleina 00 00 00, niin protocol ID:n arvo saadaan EtherType-tunnuksen määrittelemästä taulukosta kyseiselle protokollalle. EtherType-tunnuksen mukaisesti esimerkiksi Ipv4-protokollan ID on 0x0800 (kuva 3).

Muussa tapauksessa protocol ID:n määrittelee OUI:n perusteella kyseinen organisaatio. [1;3;5.]

LLC			SNAP				
AA	AA	03	00	00	00	08	00
			OUI			Protocol ID	

Kuva 3. LLC/SNAP-kehys

2.3 802.11 MAC -kerros

802.2 LLC -kerroksen alla sijaitsee 802.11 MAC -alikerros (Medium Access Control Layer). Kerroksen määrittelee vuoronvaraus CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) -protokolla, joka poikkeaa Ethernetistä sillä, että siinä on törmäysten havaitseminen korvattu niiden välttämisellä. [2.]

MAC-alikerroksen tärkeimpänä tehtävänä on hallita ja säilyttää yhteydet 802.11-asemien (esimerkiksi WLAN-päätelaite ja tukiasema, AP) välillä

koordinoimalla pääsyn jaetulle ilmatielle ja käyttämällä protokollia, jotka parantavat liikenneyhteyksiä langattomassa verkossa.

CSMA/CA-vuoronvarausta käyttämällä voidaan ehkäistä ”Hidden node” -ongelma. ”Hidden node” -ongelma aiheutuu kun kaksi WLAN-päätelaitetta kuulevat tukiaseman (AP) lähetyksen, mutta eivät kuule toisiaan päätelaitteiden etäisyydestä johtuen, jolloin päätelaitteiden välinen signaali vaimenee liikaa. Tämä ongelma esiintyy varsinkin kuormitetuissa verkoissa.

Ennen pakettien lähettämistä CSMA/CA-vuoronvarausta käyttävä lähetin kuuntelee AP:n lähettämää kanavaa käyttäen virtuaalista kantoaallon kuuntelua (Virtual Carrier Sense). Jotta päätelaitteet eivät lähettäisi samaan aikaan, pyytää päätelaite ensin lähetysluvan AP:lta RTS-sanomalla (Request to Send). Kun solu on vapaa, niin AP lähettää hyväksynnän CTS-sanomalla (Clear to Send). Hyväksynnän jälkeen päätelaite lähettää datansa joko yhdessä tai useammassa kehyksessä. Vastaanotto varmistetaan kuittaamalla jokainen datakehys erikseen. Jokainen sanoma sisältää verkonvarausvektorin (NAV, Network Allocation Vector), jolla määritellään, missä ajassa kehyksen tulee olla lähetetty. Kun NAV on viritetty, laite ei saa lähettää sanomia.

Jokaisen lähetetyn kehyksen välillä on erimittaisia viiveitä, kun ne lähetetään kanavalle. Kahden kehyksen välillä voi olla seuraavantyyppisiä viiveitä:

SIFS, Short Inter Frame Space, on viiveistä lyhin, ja se kestää 28 µs. Tätä viivettä käytetään esimerkiksi datakehyksen ja kuittauksen välillä. Mikäli kuittausta ei kuulu tämän ajan sisällä, oletetaan, että sanoma on törmännyt tai vääristynyt.

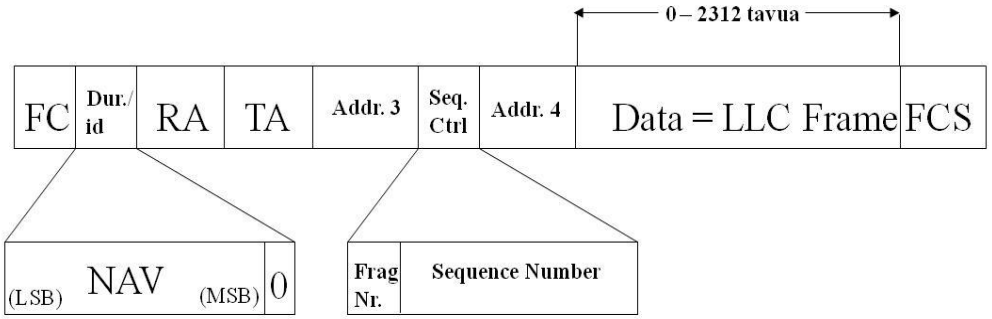
PIFS, Point Coordination IFS, on AP:n käyttämä 78 µs:n viive. Viiveen pituuden takia AP pystyy aina ottamaan käyttöönsä vapaan siirtotien ennen muita verkossa olevia laitteita. PIFS on SIFS + 1 aikaväli (Time Slot). Aikaväli on 50 ms.

DIFS, Distributed Coordination IFS, on viive, jonka päätelaite odottaa ennen kuin se voi lähettää sanoman, lisäksi NAV-ajastimen pitää olla lauennut. DIFS on SIFS + 2 aikaväliä. Lisäksi asema odottaa satunnaisen asemakohtaisen odotusajan, Back-off timen, jonka arvo on aikaväli kerrottuna satunnaisella kokonaisluvulla N. Mikäli kahdella päätelaitteella on sama kokonaisluku ja ne aloittavat lähetyksen samaan aikaan toisistaan tietämättä, tapah-

tuu törmäys. Aluksi kokonaisluku arvotaan 0-31:n väliltä, mutta kunkin törmäyksen jälkeen väli kaksinkertaistuu aina 1023:een asti. [4;5;6.]

2.3.1 MPDU-kehys

802.11 MAC-alikerros kehystää LLC-kehyksen MAC-tietosähkeeksi, MPDU:ksi (MAC Protocol Data Unit), jonka rakenne on esitetty kuvassa 4.



Kuva 4. MPDU-kehys

Frame Control, FC, 16-bittinen kehyksen ohjaus, kertoo 802.11-protokollan versiotiedon, sanoman tyypin (hallinta, ohjaus ja data) ja alityypin, onko kehys menossa vai tulossa jakelujärjestelmään, seuraako kehystä lisää sirpaleita (More Fragments), onko kyseessä kehyksen uudelleenlähetys, vaihtaako lähettäjä tehonsäästötilaan, käytetäänkö WEP-suojausta, lähettääkö AP kehyksiä torkkuvalle päätelaitteelle ja halutaanko käyttää tiukkaa kehysten (Strictly-Ordered) järjestysseurantaa.

Kesto/tunnus-kenttä (Duration/id) sisältää joko sanoman keston mikrosekunteina alkaen sanoman alusta ja päättyen sanoman kuittaukseen. Kesto siirretään NAV-ajastimeen ja sen tulee kattaa se aika, jonka tapahtuma vielä kestää alkaen tästä sanomasta. Toinen vaihtoehto on, että kenttä sisältää päätelaitteen AID-tunnuksen (Association ID), jonka se lähettää AP:lle, kun päätelaite tulee aktiiviseksi eli herää tehonsäästötilasta.

Osoitekentät koostuvat 3-4:stä osoitteesta, jotka sisältävät radiotien ja varsinaisen lähettäjän ja vastaanottajan osoitteet. Osoitekenttien sisältö riippuu siitä, minkä tyyppinen verkko (tietokoneiden välinen yhteys, Ad-Hoc, vai infrastruktuuri eli päätelaitteen ja AP:n välinen yhteys) on käytössä, meneekö sanoma AP:lle vai lähteekö se AP:lta ja onko kyseessä useampien tukiasemien muodostama silta.

Osoite 1 on aina vastaanottajan osoite DA (Destination Address) tai RA (Receiver Address). Vastaanottajan osoitteena on joko päätelaitteen 48-bittinen MAC-osoite tai AP:n solun tunniste (Basic Service Set ID, BSSID). **Osoite 2** on aina sanoman lähettäjän osoite SA (Source Address) tai TA (Transmitter Address). **Osoite 3** on sanoman alkuperäinen lähettäjän osoite, SA, kun sanoma tulee AP:lta. Jos sanoma tulee AP:lle, on osoite 3 alkuperäinen vastaanottajan osoite, DA. **Osoite 4** otetaan käyttöön, kun AP:t yhdistetään toisiinsa langattomasti eli sillataan. Tällöin osoitteet 1 ja 2 sisältävät vastaanottavan ja lähettävän AP:n tunnukset ja osoitteissa 3 ja 4 on sanoman lopullisen vastaanottajan ja lähettäjän MAC-osoitteet. Seuraavassa taulukossa on katettu kaikki eri vaihtoehdot.

Taulukko 1. MPDU –kehysten osoitekenttien käyttö

	Osoite 1	**Osoite 2**	**Osoite 3**	**Osoite 4**
Ad-Hoc	DA	SA	BSSID	-
AP:lta	DA	BSSID	SA	-
AP:lle	BSSID	SA	DA	-
Silta	RA	TA	DA	SA

Sekvenssikontrolli, Sequence Control, koostuu kahdesta osasta: 4-bittisellä (Fragmentation Number) yksilöidään pirstoumat ja 12-bittisellä järjestysnumerolla tunnistetaan pilkotun LLC/SNAP-kehyksen osat. Näin alkuperäinen data voidaan koota oikeaan järjestykseen. Numeron avulla voidaan myös havaita puuttuvat sanomat ja eliminoida virheiden aiheuttamat monistumiset.

Datakenttä sisältää LLC-kehyksen tai sen osan. Datakentän suurin pituus on 2304 tavua, jos se siirretään salaamatta ja 2312 tavua, jos siirrettävä tieto salataan. Luotettavuussyistä LLC-kehys saatetaan pilkkoa useaksi pienemmäksi osaksi.

Tarkistussumma, FCS (Frame Check Sequence), varmistaa kehyksen virheettömyyden. Se lasketaan CRC:n (Cyclic Redundancy Check) jakojään-

nösmenetelmällä, ja se kattaa sekä MAC-otsikon että datan. Samaa polynomia käytetään myös Ethernet-lähiverkoissa. [1;3;4;6.]

2.3.2 Fyysinen kerros

Fyysinen kerros (Layer 1) on myös jaettu kahteen alikerrokseen, joista ylempänä sijaitsee konvergenssiprotokolla (Physical Layer Convergence Protocol, PLCP). Tämä protokolla määrittää bittinopeudet ja fyysiset siirtotiet yhdeksi palveluksi. Alimpana sijaitsee fyysinen mediasta riippuva kerros (Physical Medium Dependent, PMD). Tässä kerroksessa määritellään kanavointitapa, modulaatio ja hajaspektritekniikan toteutus. Eri standardien suorituskyvyt määritellään tässä kerroksessa. Fyysisestä kerroksesta puhutaan lisää myöhemmissä kappaleissa, kun standardeihin perehdytään tarkemmin. [2.]

3 IEEE 802.11 -STANDARDIN KEHITYS

Ensimmäinen WLAN-standardi, IEEE 802.11, tuotiin markkinoille 1997. Jo standardin kehitysvaiheessa kuitenkin huomattiin, että siirtonopeus ei riitä houkuttamaan käyttäjiä Ethernet-lähiverkoista. Lisäksi yhteensopivuuden vajavuudet sekä taajuusalueisiin liittyvät lupaongelmat aiheuttivat käyttäjissä haluttomuutta siirtyä käyttämään standardia. IEEE 802.11 antoi kuitenkin hyvän pohjan kehitykselle. [2.]

3.1 IEEE 802.11 -standardi

Alkuperäinen standardi sisältää taajuushyppelyhajaspektrin, FHSS (Frequency Hopping Spread Spectrum) ja suorasekvenssihajaspektri, DSSS (Direct Sequence Spread Spectrum) fyysiset kerrokset 2,4 GHz:n taajuuskaistalla. Standardi tarjoaa joko 1 tai 2 Mbps siirtonopeuden. Seuraavaksi käydään läpi molemmat yhteystavat.

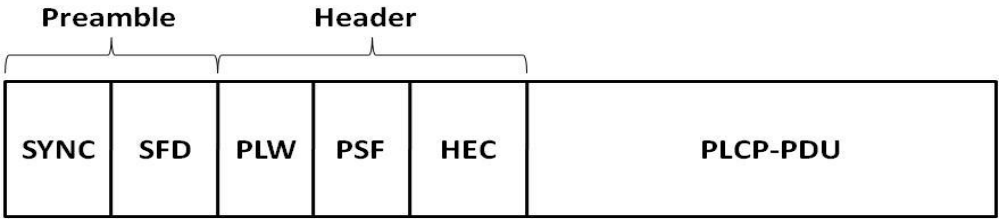
3.1.1 FHSS

FHSS lähettää laajakaistasignaalia, joka kattaa koko 2,4 GHz:n kaistan. FHSS käyttää GFSK-modulointia (Gaussian Frequency Shift Keying) saavuttaakseen siirtonopeudet, 2-GFSK:ta 1 Mbps:lle ja 4-GFSK:ta 2 Mbps:lle. Taajuushyppely jakaa bittivirran paketteihin jotka lähetetään purskeina (burst) käyttäen eri kantoaaltotaajuuksia. FHSS:tä käyttävät AP:t voidaan säätää toimimaan jopa 15 eri hyppelykuvion mukaan, mikä mahdollistaa 15 FHSS-AP:n toimimisen samalla alueella. [2.]

Kuten edellisessä kappaleessa mainittiin, fyysinen kerros koostuu PLCP:stä ja PMD:stä. FHSS:n fyysisessä kerroksessa määritellään kolme kokonaisuutta:

- PMD-alikerros, toimittaa siirtorajapinnan lähettävän ja vastaanottavan aseman välille.
- LME (Layer Management Entity), pitää huolen paikallisen fyysisen toiminnon hallinnasta yhdessä MAC-hallintakokonaisuuden kanssa.
- PLCP-alikerros, selkeyttää MAC-kerroksen ja fyysisen kerroksen välisen rajapinnan.

PMD hoitaa siis kehysten lähettämisen ja vastaanoton ja LME auttaa synkronoimalla taajushyppelysekvenssin kaikkien verkon asemien välillä. PLCP-kerros toimittaa rajapinnan MAC-kerroksen kanssa ja mukauttaa MPDU-paketin PLCP-kehykseksi lähetystä varten. Kuvassa 5 nähdään kehyksen koostumus.



Kuva 5. PLCP-kehysrakenne (FHSS)

PLCP alkumerkki, preamble, ja otsikko, header, lähetetään aina 1 Mbps nopeudella, mutta PLCP-PDU (PLCP- Protocol Data Unit) voidaan lähettää joko 1 Mbps:n tai 2 Mbps:n nopeudella.

Kehys koostuu seuraavista osista:

SYNC on 80-bittinen vaihteleva sekvenssi nollia ja ykkösiä, joka alkaa 0:lla ja päättyy 1:een. Se kertoo vastaanottajalle saapuvasta signaalista ja sallii vastaanottajan synkroida kantoaallon ja kellon sekä valita antennin, jos käytetään monitaajuusmenetelmää.

Start frame delimiter (SDF) on 16-bittinen viesti, joka mahdollistaa kehyksen synkroinnin. Se on muotoa 0000 1100 1011 1101.

PLCP-PDU length word (PLW) on 12-bittinen viesti, joka kertoo MPDU-paketin oktettien määrän, joka voi olla välillä 0-4095.

PLCP-PDU Signaling field (SLF) koostuu 4 bitistä, joista ensimmäinen on varattu tuleville sovelluksille. Jälkimmäiset kolme ilmoittavat bittinopeuden, 000 tarkoittaa 1 Mbps ja 010 tarkoittaa 2 Mbps.

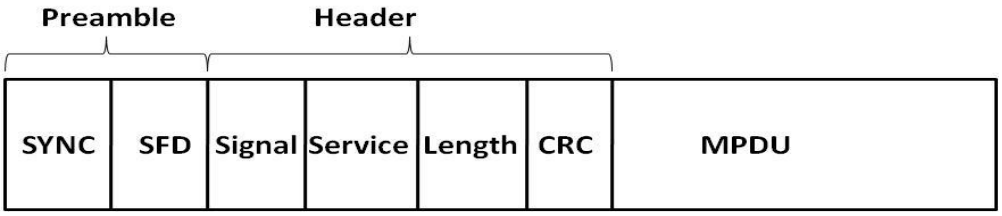
Header Error Check (HEC) on 16-bittinen virheentarkistus.

PLCP-PDU sisältää MPDU:n tiedot sekoitettuna ja käsittelemättönä. Data sekoitetaan käyttämällä 127 bittistä synkronista signaalin sekoitinta. [2;3;5.]

3.1.2 DSSS

DSSS käyttää BPSK-modulaatiota (Binary Phase Shift Keying) saavuttaakseen 1 Mbps:n nopeuden ja nelivaiheista QPSK-modulaatiota (Quadrature PSK) 2 Mbps:n nopeudelle. DSSS yhdistää lähetettävään dataan chip-sekvenssin, jotta saadaan uusi bittijärjestys 11Mchip/s nopeudella. Tällä sekvenssillä moduloidaan kantoaalto.

DSSS:n käyttämä PLCP-kehys eroaa hieman taajuushyppelyn käyttämästä. Seuraavaksi käydään se läpi (kuva 6).



Kuva 6. PLCP-kehysrakenne (DSSS)

SYNC, 128-bittinen sarja ykkösiä tarjoaa kaiken synkronisointiin tarvittavan tiedon.

SFD, 16-bittinen viesti F3A0H.

SIGNAL, 8-bittinen kenttä, joka kertoo, mitä modulointia käytetään. 0AH kertoo että siirtonopeus 1 Mbps ja 14H kertoo, että nopeus on 2 Mbps.

SERVICE, tämä kenttä on varattu tulevia sovelluksia varten, arvo 00H kertoo että laite on 802.11-standardiin soveltuva.

LENGTH, 16-bittinen kokonaisluku, kertoo kuinka monta mikrosekuntia MPDU-paketin lähetys kestää.

CRC (Cyclic Redundancy Check), CRC 16-polynomigeneraattori virheen estämiseen PLCP-otsikkotiedossa.

MPDU-kenttä sisältää kaiken MPDU-paketin datan samassa järjestyksessä.

Ennen lähetystä kaikki PLCP-kehyksen bitit sekoitetaan itse-synkronoidulla sekvenssillä, joka on 127-bittinen. Sekoitus alkaa kehyksen alussa, kun viesti on mikä tahansa muu paitsi kaikki 0:ia.

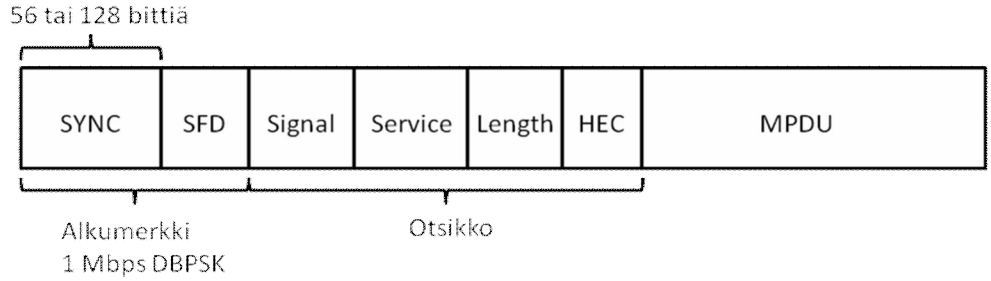
Alkuperäisen 802.11-standardin jälkeen on markkinoille julkaistu IEEE 802.11b-, 802.11a- ja 802.11g-standardit. Kuten mainittu, 802.11-standardien erot tulevat esille fyysisessä kerroksessa, seuraavaksi käsittelemmekin kolmea edellä mainittua standardia fyysisen kerroksen osalta ja käymme läpi niiden ominaisuuksia. [4;5.]

3.2 IEEE 802.11b –standardi

Syksyllä 1999 IEEE julkaisi 802.11b-standardin, siinä määriteltiin aiempien 1 ja 2 Mbps:n lisäksi nopeammat siirtoyhteysnopeudet 5,5 Mbps ja 11 Mbps samalla 2,4 GHz:n taajuudella. Standardista käytetään myös nimeä 802.11hr (high rate). Standardi käyttää jo alkuperäisestä 802.11-standardista tuttua suorasekvenssihajaspektritekniikkaa ja samaa PLCP-otsikkorakennetta ja on täten alaspäin yhteensopiva alkuperäistä 802.11 DSSS-standardia käyttävien laitteiden kanssa. [2.]

3.2.1 PLCP-konvergenssikerros

Konvergenssikerros lisää MPDU-kehyksiin omat PLCP-PDU-otsikkonsa. 802.11b:n PPDU-kehyksiä on olemassa pitkä ja lyhyt, ja ne molemmat sisältävät alkumerkin, otsikon ja datakentät. Kuten aiemmassakin standardissa, alkumerkki lähetetään aina 1 Mbps:n nopeudella käyttäen DBPSK-modulaatiota. Seuraavassa käydään läpi 802.11b:n PPDU-kehys (kuva 7).



Kuva 7. 802.11b PPDU-kehysrakenne

Alkumerkki koostuu SYNC- ja SFD-kentistä. Synkronointikentän tehtävänä on synkroida lähettävä ja vastaanottava asema toisiinsa, säätää vastaanottokello ja auttaa valitsemaan parhaan signaalin antava signaali. Synkronointimerkki voi olla joko 128 tai 56 bittiä pitkä bittikuvio. SFD-kenttä erottaa alkumerkin ja kehyksen toisistaan.

Alkumerkin jälkeen seuraa PPDU:n otsikko, joka lähetetään joko 2 Mbps:n nopeudella käyttäen DQPSK-modulaatiota (Differential Quadrature Phase Shift Keying) kun kyseessä on lyhyt kehys ja 1 Mbps:n nopeudella käyttäen DBPSK-modulaatiota (Differential Bipolar Phase Shift Keying), jos kyseessä on pitkä kehys. Kehys sisältää molemmissa tapauksissa seuraavat otsikkokentät:

- Signaali (PLCP Signaling) ilmoittaa, millä bittinopeudella datakenttä siirretään.

- Palvelukentän (Service) 3 bittiä otettiin käyttöön 802.11b:ssä. Ne sisältävät pituuskentän 17. bitin, tiedon käytetystä moduloinnista (CCK, Convolutional Code Keying tai PBCC, Packet Binary Convolutional Coding) ja kellon lukituksesta. Kellon lukitus tarkoittaa, että lähetin ja symbolikello käyttävät samaa värähtelijää.

- Pituuskenttä (Length) kertoo kehyksen lähettämiseen tarvittavan ajan mikrosekunneissa.

- Otsikon tarkistussumma (Header Error Check, HEC) varmentaa PPDU -kehysotsikon virheettömyyden, mutta se ei havaitse muualla kehyksessä olevia virheitä. Lähetys tapahtuu 2 Mbps:n bittinopeudella, jos se on mahdollista.

Viimeisenä kehyksessä on datakenttä, joka sisältää MPDU –kehyksen. Se lähetetään signaalikentän määrittelemällä nopeudella käyttäen bittinopeuden mukaista modulointia. Koko kehys sekoitetaan ennen hajotusta. Sekä lähetin että vastaanotin käyttävät samaa polynomia sekoitukseen, joten sekoitus ei vaikuta kehykseen tai sen siirtämään dataan. [1;6;7.]

3.2.2 Fyysinen mediariippuva kerros, PMD

Fyysisessä mediariippuvassa kerroksessa määritellään eri standardit, bittinopeudet, bittien hajoitus alikanaville ja modulaatiotavat. Nykyisin käytetään lähes ainoastaan radiolähetystä ja hajaspektritekniikkaa, joka tarkoittaa että lähetys hajautetaan kantoaallon molemmille puolin tarvittua laajemmalle alueelle kuin mitä bittinopeus edellyttäisi. Tämä sen vuoksi, ettei vapailla taajuuksilla esiintyvät häiröt vaikuttaisi koko lähetysspektriin. 802.11b-verkoissa

käytetään Barker- tai CCK-hajautusta riippuen bittinopeudesta. Kanavan taajuusalue on kaikissa tapauksissa 22 MHz:ia.

Kun data lähetetään 1:n tai 2 Mbps:n nopeuksilla käytetään Barker-hajautusta, jossa lähetettävät bitit lasketaan binaarisesti yhteen yhdentoista bitin Barker-koodin kanssa, josta saadaan lähetettävä bittijono, jossa on 11 alkiota (Chip) kustakin databitistä. Vastaanottajan puolella lasketaan alkiojono yhteen Barker-koodin kanssa, jolloin saadaan alkuperäiset databitit. Barker-koodi on valittu siten, että se muistuttaisi näennäissatunnaista kohinaa. Tämä siksi, ettei se häiritsisi muita järjestelmiä. 11-bitin Barker-koodi on 10110111000. 2 Mbps:n bittinopeuksiin päästään, kun moduloidaan kaksi bittiä yhtä signaalielementtiä kohti.

Ylemmillä bittinopeuksilla käytetään CCK–hajautusta eli komplementaarikoodiavainnusta. CCK-hajautuksessa käytetään ensin 11-bitin hajautusta. Sen jälkeen alkiobitit jaetaan kahdeksan alkion koodisanoiksi eli symboleiksi. Mahdollisesta 256 sarjasta valitaan vain muutama, jolla koodataan neljän tai kuuden bitin sanoja. Koodisanat valitaan siten että vastaanottajan on helppo erottaa ne toisistaan myös häiriöllisissä olosuhteissa. Symbolikello on ylemmillä nopeuksilla 1,375 Msym/s.

5,5 Mbps:n nopeudella alkiovirrasta eroitetaan 4 bitin blokkeja, joista 2 koodataan DQPSK -vaihe-erolla ja loput 2 bittiä sopivasti valituilla kahdeksan bitin koodisanoilla. 11 Mbps:n nopeuksilla eroitetaan alkiovirrasta 8 bitin blokkeja joista 2 bittiä koodataan DQPSK-vaihe-erolla ja loput 6 bittiä käyttäen 8 bitin koodisanoja.

Euroopassa 802.11b käyttää ETSI:n (European Telecommunications Standards Institute) määrittelemää vapaata taajuusaluetta 2,4-2,485 GHz:n välillä. Alue on jaettu 13:sta kanavaan ja niiden väli on 5 Mhz, kanavan kaistanleveys on 22 Mhz joten käytettävissä on vain kolme ei-päällekkäistä kanavaa: 1, 7 ja 13. Yhdysvalloissa on FCC:n (Federal Communications Commission) määräyksestä käytössä vain 11-kanavaa, jolloin ei-päällekkäisiä kanavia on 1, 6 ja 11. Taajuusalue on 2,4-2,475 GHz. [1.]

Vuoden 1999 lopulla, samoihin aikoihin 802.11b:n kanssa, julkaistiin toinenkin standardi, 802.11a. Standardi toimii 5 GHz:n taajuusalueella ja käyttää OFDM -tekniikkaa. Lähes samoilla ominaisuuksilla, tosin 2,4 GHz:n taajuus-

alueella, toimiva 802.11g julkaistiin 2003. Seuraavaksi käydään nämä standardit tarkemmin läpi. [8;9.]

3.3 IEEE 802.11a- ja 802.11g-standardit

Tarve saada langattomien lähiverkkojen nopeudet vastaamaan Ethernetin nopeutta, IEEE julkaisi 1999 korkeammalla 5 GHz:n alueella toimivan 802.11a-standardin. Se julkaistiin periaatteessa ennen 802.11b:tä, siksi se nimettiin 802.11a:ksi. Yhdysvalloissa se käyttää U-NII (Unlicensed National Information Infrastructure) kaistoja 5.15-5.25 GHz, 5.25-5.35 GHz, ja 5.725-5.825 GHz. Euroopassa 802.11a sai vasta vuoden 2002 puolivälissä luvan käyttää vapaata ylempää ISM (Industrial, Scientific and Medical) -taajuusaluetta 5.725-5.875 GHz:n välillä. [11;12]

802.11a määriteltiin käyttämään tiedonsiirtoa varten OFDM (Orthogonal Frequency Division Multiplexing) -tekniikkaa, jossa signaali jaetaan 52:en pienempään alasignaaliin, jotka lähetetään samanaikaisesti eri taajuuksilla käyttäen joko BPSK-, QPSK- tai QAM -modulaatiota. Taajuutta nostamalla ja verkkotekniikkaa muuttamalla saatiin bittinopeus nostettua maksimissaan 54 Mbps:ssa, mutta samalla jouduttiin luopumaan yhteensopivuudesta aiempien standardien kanssa koska ne toimivat eri taajuusalueella. [11.]

802.11g ratifioitiin IEEE:n toimesta vuonna 2003, se on 802.11b:n laajennus jossa periaatteessa risteytettiin 802.11b ja 802.11a. Se käyttää 2,4 GHz:n taajuusaluetta, tarjoaa yhteensopivuuden 802.11b-standardia käyttävien laitteiden kanssa ja mahdollistaa 54 Mbps:n siirtonopeuden käyttämällä 802.11a:ssa esiteltyä OFDM-tekniikkaa. [10;12.]

Seuraavassa osiossa käydään läpi OFDM:n fyysinen kerros, joka on lähes sama molemmissa standardeissa.

3.3.1 OFDM:n fyysinen kerros

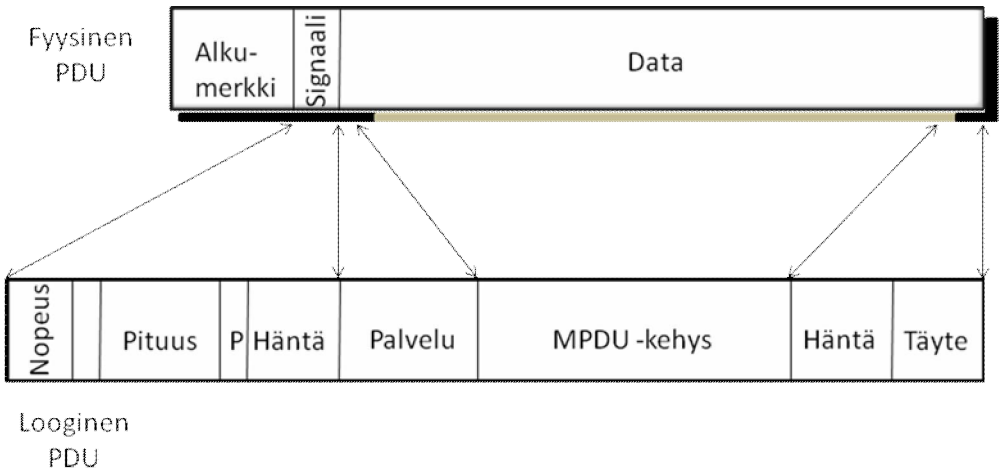
Monikantoaaltomodulointi, OFDM, jakaa siirrettävän datan eri taajuuksisiin alikanaviin jotka siirretään rinnakkain. 802.11a ja 802.11g käyttävät eri taajuusalueita, mutta tekniikka on sama.

OFDM ei käytä alikanavien välissä varokaistaa (Guard Band) vaan taajuusalue jaetaan kanaviin niin että kunkin kanavan keskitaajuudella muiden kanavien spektri on nolla. Alikanavien spektrit ovat toisistaan riippumattomia eli

ortogonaalisia. OFDM:ssä lähetin muodostaa alikanavista lähetettävän signaalin käyttämällä käänteistä nopeaa Fourier-muunnosta (IFFT), ja vain lähetetyssignaalin spektrillä on merkitystä. Vastaanotin käyttää nopeaa käänteistä Fourier-muunnosta (FFT) laskeakseen alikanavien taajuusspektrien amplitudit ja muodostaa alikanavien tiedoista alkuperäisen bittijonon. [1;11;12.]

3.3.2 OFDM-konvergenssikerros

Konvergenssikerros käyttää PPDU-kehystä kuvan 8 mukaisesti.



Kuva 8: OFDM PPDU –kehys fyysisellä ja loogisella tasolla

Kuvasta 8 nähdään, että konvergenssikerroksen PPDU-kehys muodostuu alkumerkistä (Preamble) ja otsikosta.

- Alkumerkki koostuu 12 OFDM-symbolista. Nämä synkronoivat lähettimen ja vastaanottimen ajastimet, ensimmäiset kymmenen symbolia, joita kutsutaan lyhyiksi koulutussekvensseiksi, auttavat automaattisen vahvistuksen säädön ja taajuuserojen arvioinnissa. Loput kaksi symbolia, pitkät koulutussekvenssit, hoitavat hienosäädön.

- Otsikko koostuu yhdestä symbolista, signaalikentästä. Se koostuu 4 bitin hyötykuorman nopeuskentästä, varatusta bitistä, 12 bittisenä ilmoitetusta MAC-kehyksen pituudesta, pariteettibitistä, jota käytetään otsikon tietojen salaamiseen sekä 6 bittisen hännän, joka pitää huolen, että konvoluutiokooderi on tyhjennetty otsikon koodauksen jälkeen (sisältää pelkkiä 0-bittejä).

- Looginen PPDU-otsikko sisältää myös 16 bittisen palvelukentän ja vaihtuvamittaisen loppumerkin, jotka lainataan fyysisen kehyksen datakentästä. Datakentän bitit, myös palvelukenttä, sekoitetaan (scramble) ennen lähetystä.

- Myös loppumerkin bitit lainataan datakentästä. Se sisältää kuuden bitin loppumerkin, joka lopettaa konvoluutiokoodauksen sekä vaihtuvamittaisen täytteen (Padding), jolla täytetään datakenttä OFDM:n tarvitsemaan lohkopituuteen. [1;11;12.]

3.3.3 OFDM PMD

Fyysisellä mediariippuvalla kerroksella lähetetään 250 000 symbolia sekunnissa käyttäen 48 alikanavaa. Bittinopeus määräytyy virheenkorjaukseen uhrattavista biteistä ja modulaatiotavasta. Korkeimman mahdollisen nopeuden saa käyttämällä 64-QAM-modulointia ja virheenkorjauksen konvoluutiosuhdetta 3/4. Tällöin 6 bittiä koodataan yhteen merkkiin, kun kaikki 48 alikanavaa lähettävät rinnan saadaan 288 bittiä. Biteistä 1/4 käytetään virheenkorjaukseen ja 3/4 datalle saadaan 216 bittiä kutakin symbolia kohti. Tästä saadaan 216b * 250000 1/s = 54 Mbps.

Taulukko 2. OFDM-siirron moduloinnit, virheenkorjaussuhteet ja bittinopeudet

Mbps	**Modulaatio**	**Bittejä/ kantoaalto**	**Bittejä/ symboli**	**Koodaus-suhde**	**Databittejä/ symboli**
6	BPSK	1	48	1/2	24
9	BPSK	1	48	3/4	36
12	QPSK	2	96	1/2	48
18	QPSK	2	96	3/4	72
24	16-QAM	4	192	1/2	96
36	16-QAM	4	192	3/4	144
48	64-QAM	6	288	2/3	192
54	64-QAM	6	288	3/4	288

Yhteensopivuussyistä 802.11g sisältää myös CCK-koodauksen sekä 5,5 ja 11 Mbps:n bittinopeudet. Vanhemman 802.11b-standardin käyttö samanaikaisesti 802.11g-laitteiden kanssa hidastaa koko verkkoa koska 802.11b:tä käyttävät laitteet saattavat varata kanavan kehyksen lähetyksen ajaksi. Aika saattaa olla kymmenkertainen 802.11g:n nopeimpaan bittinopeuteen nähden. [1;2.]

3.4 802.11a VS. 802.11g

Kuten on jo selville tullut, ainoana suurena erona on se, että 802.11a käyttää Yhdysvalloissa vapaasti käytettäviä U-NII:n 5 GHz:n taajuusalueita ja 802.11g ISM:n määrittämää 2,4 GHz:n taajuusaluetta Euroopassa. Muita eroja ovat:

- 802.11a:n taajuusalueen vuoksi radioaaltojen vaimennus on suurempaa ja siten kantomatka noin 60 % siitä mitä 802.11g:llä. Tästä johtuu myös suuremman lähetystehon ja tehonkulutuksen tarve.
- Yhteensopivuus aiempia standardeja käyttävien laitteiden kanssa puuttuu kokonaan 802.11a:sta.
- 802.11a-laitteilla on korkeat hinnat.
- 802.11g toimii samalla taajuusalueella mikroaaltouunien, bluetooth-laitteiden ja langattomien puhelinten kanssa, joten ilmatie saattaa ruuhkautua.
- 802.11a:ssa on 12 ei-päällekkäistä kanavaa kun taas 802.11g:ssä on vain 3.

[10.]

Markkinoille on tullut jo nyt tulevaan IEEE 802.11n -vedoksiin perustuvia laitteita jotka lupaavat jopa 300 Mbps:n nopeuksia. Standardia ei ole vielä ratifioitu, joten sitä ei käsitellä tässä työssä enempää.

4 IEEE 802.16 –STANDARDI: BROADBAND WIRELESS ACCESS, BWA

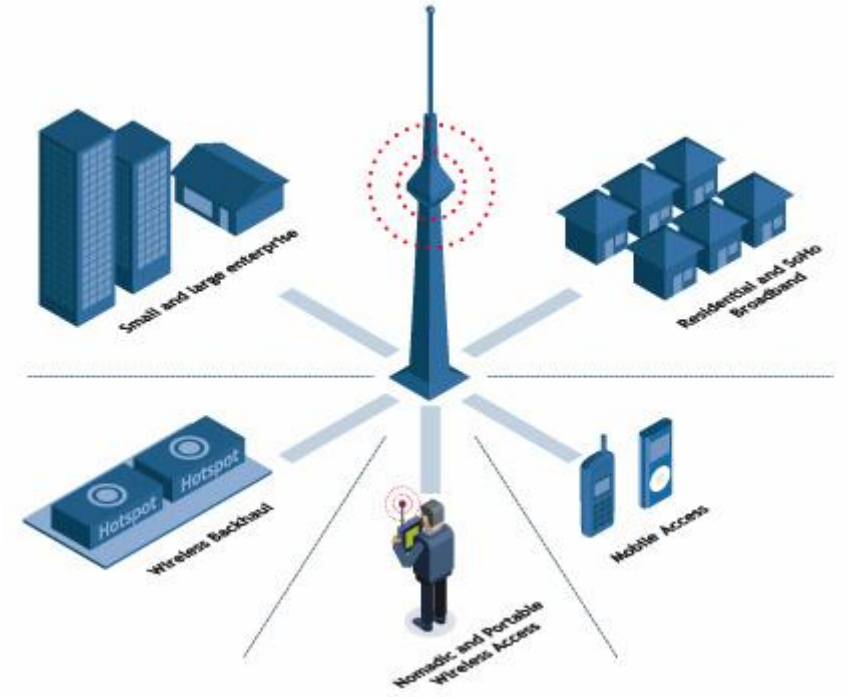
Vuonna 1999 IEEE 802.16 -työryhmä alkoi suunnitella laajakaistaista langatonta kaupunkialueverkkoa, jossa niin kutsuttu ”viimeinen maili” eli tilaajayhteyskaapeli korvattaisiin langattomalla yhteydellä. Ensimmäinen standardi julkaisiin 2001, mutta sen kehitys jatkui ja jatkuu edelleen. Standardia kutsutaan yleisimmin nimellä WiMAX (Wireless Microwave Access). Nimitys tulee WiMAX Forum™ organisaation mukaan. WiMAX Forum™ on telealan yhteishanke, jonka tavoitteena on nopeuttaa IEEE 802.16 -standardiin perustuvien langattomien laajakaistaverkkojen käyttöönottoa. Foorumi määrittelee ja verifioi standardeja IEEE 802.16 -standardin pohjalta.

IEEE hyväksyi ensimmäisen 802.16-standardin langattomalle kaupunkialueverkolle joulukuussa 2001 taajuusalueelle 10-66 GHz, ja se julkaistiin 2002. Tammikuussa 2003 802.16a:ssa määriteltiin 2-11 GHz:n taajuusalue ja standardiin on tullut lähes vuosittain lisäyksiä, viimeisin 802.16e julkaistiin joulukuussa 2005. Se toi erona aiempiin standardeihin mobilititeetin, joka mahdollistaa päätelaitteen liikkumisen tukiasemasta toiseen. [13.]

IEEE 802.16 kehitettiin korvaamaan kaapelimodeemi ja DSL yhteydet hajaasutusalueilla, joissa ei ole valmiiksi vedettyjä kaapeleita. Kaapeliverkon rakentaminen tulisi liian kalliiksi ja vaikeaksi joten näillä alueilla langaton yhteys on varteenotettava vaihtoehto. Yksi tukiasema tuo teoreettisesti optimaalisissa olosuhteissa yhteyden 50 kilometrin säteelle lähettimestä, mutta käytännössä yhteydet yli 20 kilometrin etäisyyksillä vaativat suoran näköyhteyden (LOS, Line of Sight). Operaattorit lupaavat 10 Mbps 10 km:n säteellä. Sade, sumu ja fyysiset esteet vaikuttavat kantamaan. [14.]

Standardin uusin lisäys, 802.16e toimii Euroopassa alle 3,5 GHz:n taajuudella ja Yhdysvalloissa 2,5 GHz:n ja 5,8 GHz:n taajuudella. Lisäyksessä on määritelty käytettäväksi mukautuvaa OFDM–modulointia (Scalable OFDM, SOFDM), joka ei ole suoraan yhteensopiva aiempien lisäysten kanssa. MAC-suojauskerros hoitaa autentikoinnin ja salauksen, autentikointi on toteutettu PKM-EAP:lla (Public Key Method-Extensible Authentication Protocol), jossa käytetään jokaisessa päätelaitteessa olevaa yksilöllistä X.509-sertifikaattia sekä RSA-avaimenvaihtoalgoritmia. Liikenteen salaus ja purku toteutetaan käyttäen joko AES- (Advanced Encryption Protocol) tai DES3 (Data Encryption Standard 3) -standardia. [13;14.]

Seuraavassa kuvassa joitain 802.16-standardin käyttötapoja:



Kuva 9. IEEE 802.16 käyttötavat

Haja-asutusalueiden lisäksi muita käyttäjiä ovat esimerkiksi pienet ja suuret yritykset, pien- ja kotitoimistot ja kaupunkialueet, joissa asiakkaat voivat käyttää yhteyttä kaupungilla liikkuessaan. WiMAX voi toimia myös WLAN-HotSpottien runkoyhteytenä. Yrityksissä WiMAX voisi toimia varayhteytenä, se vaatisi vain vastaanottimen josta yhteys voitaisiin ottaa käyttöön pääyhteyden katketessa tai sen kapasiteetin loppuessa.

5 IEEE 802.20: MOBILE BWA

Standardin kehittäminen on ollut vastatuulessa, koska IEEE 802.20-työryhmän jäsenet ovat olleet erimielisiä sen kannattavuudesta, ottaen huomioon edellisessä kappaleessa esitellyn WiMAX:in ja mobiilipäätelaitteille tarjottavan 3G-yhteyden, jotka periaatteessa ajavat samaa asiaa. Standardin kehittäminen keskeytettiin väliaikaisesti 8.6.2006, mutta 15.9.2006 koko työryhmän johtokunta vaihdettiin ja suunnitelma standardin kehittämisestä jatkui. [15.]

Työryhmän luonnoksen päämääränä on tarjota seuraavia etuja käyttäjille:

- tukee yhteyttä jopa 250 km/h nopeudessa
- yli 1Mbps/300 kbps siirtonopeus
- toimii lisensoidulla alle 3,5 GHz:n alueella
- suojaus käyttäen AES-protokollaa
- parempi taajuuksien hyötykäyttö, suurempi aktiivinen käyttäjämäärä ja taatumpi tiedonsiirtonopeus kuin olemassaolevilla mobiilijärjestelmillä.

IEEE-SA:n standardien johtokunta myönsi standardille kahden vuoden jatkoajan, mikä tarkoittaa että standardin tulisi olla valmis viimeistään 31.12.2008. [16.]

6 LANGATTOMIEN VERKKOJEN SUOJAUS

Suurimpana huolenaiheena langattomissa verkoissa on tiedon salaus. Suojaamattomana kaikki alueella olevat päätelaitteet voivat ottaa yhteyden tukiasemaan, käyttää yhteyttä palvelun tilaajan sitä huomaamatta tai jopa tarkastella esimerkiksi käyttäjän sähköposteja. Tässä kappaleessa käydään läpi muutamia tapoja, joilla yhteys voidaan suojata ja väärinkäyttö estää.

6.1 MAC-suodatus

Jokaisella verkkokortilla, joka käyttää verkkoa on identtinen 12 -merkkinen MAC-osoite, jonka laitteenvalmistaja on määritellyt laitteelle. Tukiasemaan on mahdollista määritellä lista MAC-osoitteista, jotka saavat käyttää yhteyttä. Muut laitteet hylätään yhteydenottohetkellä.

Suojauksen heikkoutena on se että MAC-osoitteet kulkevat salaamattomina jokaisessa langattoman verkon paketissa, vaikka niissä itse data olisikin salattu. Liikennettä kuuntelemalla siihen tarkoitetuilla ohjelmilla saa MAC-osoitteen selville muutamissa sekunneissa. Useimmissa tietokoneissa verkkokortin MAC-osoitteen saa vaihdettua helposti. Näin yhteys verkkoon aukeaa helposti. Lisäksi MAC-osoitteiden listan ylläpitäminen on työlästä varsinkin, jos verkkoon lisätään uusia koneita usein tai verkkoa tarjotaan vierailijoille. [1;2.]

6.2 Piilotettu SSID

Jokaisella tukiasemalla on verkkotunnus johon päätelaitteet liittyvät, sitä kutsutaan SSID:ksi (Service Set Identifier). Tukiasema lähettää tätä tunnusta eli ”mainostaa” omaa langatonta verkkoaan. SSID:n avulla eroitetaan samalla alueella olevat langattomat verkot. Tukiaseman asetuksissa on mahdollista määrittää lähettääkö tukiasema tätä tunnustaan, jos valitaan, että SSID piilotetaan niin alueella olevat päätelaitteet eivät automaattisesti löydä verkkoa ilman että ne tietävät SSID:n.

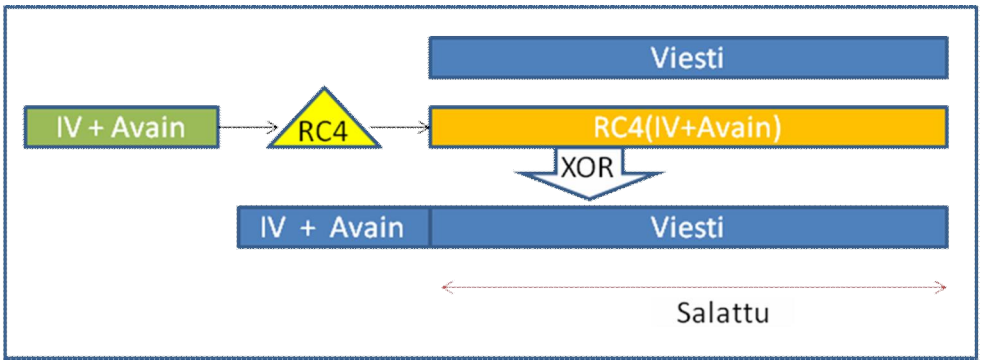
Vaikka SSID piilotetaan, niin se kuitenkin lähetetään salaamattomana verkon yli useassa muussa tilanteessa. Esimerkiksi tietokoneen kirjautuessa langattomaan verkkoon SSID kulkee salaamattomana asiakaskoneen ja tukiaseman välillä. Niinpä tarpeeksi kauan verkkoa kuuntelemalla on mahdollista saada piilotettu SSID selville. [17.]

Edellä mainitut suojausmenetelmät eivät varsinaisesti salaa verkon liikennettä. Kuka tahansa voi tarkastella verkon liikennettä, jos sitä ei ole salattu. Seuraavaksi käydään itse liikenteen salaaminen.

6.3 WEP-salaus

WEP on IEEE 802.11 -suosituksen ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä. WEP-salauksessa (Wired Equivalent Privacy) tukiasemalle määritellään salaussavain joka voi olla 64-, 128- tai 256-bittinen. Pituudesta riippuu se, kuinka kauan salauksen murtamisessa kestää eli mitä pidempi sen vaikeampi se on purkaa. [1.]

WEP käyttää RSA Securityn RC4-salausalgoritmia, 24-bittistä alustusvektoria, IV (Initialization Vector) ja 40-, 104- tai 232-bittistä salausavainta. Käytettäessä WEP-salausta verkon datapaketit salataan käyttäen jaettua salausavainta ja alustusvektoria, joka vaihtelee eri pakettien välillä. Salausavain on pituudesta riippuen 5-29 merkkiä pitkä salasana, joka on vain tukiaseman ja siihen liittyneiden tietokoneiden tiedossa. 24-bittinen alustusvektori lähetetään aina paketin otsaketiedoissa salaamattomana, jotta vastapuoli voisi purkaa paketin sisällön. RC4-salausalgoritmi luo edellä mainittujen tietojen perusteella bittijonon, jossa on myös 32-bittinen aitouden tarkistusarvo (Integrity Check Value, ICV), joka lasketaan käyttäen CRC-32:ta. Muodostetun bittijonon ja salattavan tekstin yhdistämällä XOR-operaatiolla saadaan lähetettävä salattu teksti (kuva 10). Vastapuoli osaa purkaa paketin sisällön, koska alustusvektori lähetetään selkokielisenä paketin mukana ja vastapuoli tietää jaetun salausavaimen. [18.]



Kuva 10. WEP-suojattu kehys

Salauksen purkaminen on helppoa, ja se on osoitettu useaan otteeseen. Esimerkiksi Yhdysvaltojen F.B.I on näyttänyt, kuinka WEP-salauksen purkaminen onnistuu noin 3 minuutissa hyödyntäen julkisesti käytettävissä olevia työkaluja. WEP-suojauksen ongelmana on alustusvektorien heikkous. Alkuperäisenä tarkoituksena oli etteivät selkokielisinä lähetetyt alustusvektorit toistuisi, mutta 24-bittinen alustusvektori ei riitä varsinkaan vilkkaasti liikennöidyssä verkossa. Salauksen murtamiseen tarvitsee vain kaapata tarpeeksi paketteja jotka sisältävät alustusvektorin, IV. Kun näitä heikkoja IV-paketteja on saatu kaapattua tarpeeksi, voidaan niille tehdä tilastollinen analyysi, jonka avulla pystytään selvittämään alkuperäinen salausavain. Verkkoliikennettä voidaan lisätä lähettämällä deauth-hyökkäyksiä verkossa oleville koneille, jolloin ne joutuvat ottamaan yhteyden uudelleen tukiasemaan. [18;19.]

6.4 WPA

WPA (Wi-Fi Protected Access) kehitettiin parantamaan WEP –suojauksessa havaittuja aukkoja. Se on aikaisempi versio IEEE 802.11i lisäyksestä. WPA tuen saa useimmille tukiasemille ja päätelaittelle päivittämällä niiden ohjelmiston. WPA-Personal tarjoaa suojauksen salausavaimella ja käyttää 128-bittisiä salausavaimia ja vaihtuvia istuntokohtaisia avaimia.

WPA PSK-TKIP

Pienille firmoille ja kotitoimistoille soveltuva WPA-PSK TKIP -suojaus tarjoaa vahvan suojauksen käyttäjille joilla ei ole varaa tai taitoa ylläpitää varmentavaa palvelinta. Se perustuu ennaltamääritettyyn salausavaimeen, PSK (Pre-Shared Key) ja TKIP (Temporal Key Integrity Protocol) -salausalgoritmiin, joka perustuu WEP-suojauksesta tuttuun RC4-jonosalausalgoritmiin. PSK-salausavain määritellään sekä tukiasemalle että päätelaitteelle, kuten tehtiin WEP-suojauksessakin. Sen on oltava 8-63 ASCII merkkiä tai enimmillään 64 hexadesimaalia. TKIP tuo neljä uutta algoritmia WEP-suojaukseen:

- sanoman yhtenäisyystarkistus, MIC
- alustusvektorien jaksotustarkkuus
- pakettikohtainen avainten sekoitus

- uudelleenavainnusmenetelmän

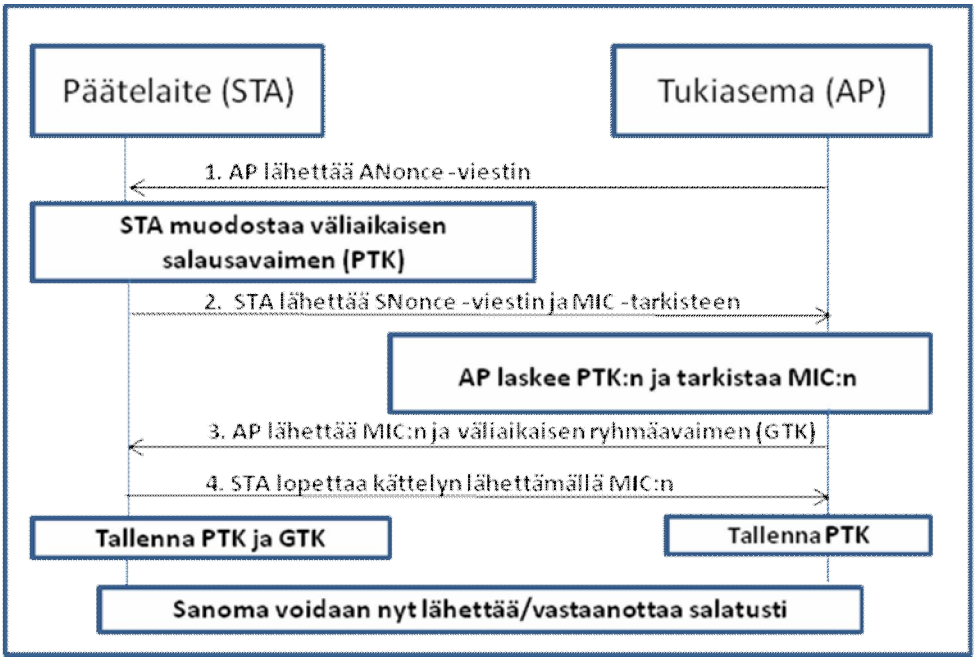
Sanoman yhtenäisyystarkistuksessa (Message Integrity Code, MIC) algoritmi tuottaa 64-bittisen tarkisteen viestin sisällöstä, viestin prioriteettitiedosta, sekä lähettäjän ja vastaanottajan osoitteista. Tarkisteen laskemisessa käytetään 64-bittistä avainta. Tällä estetään hyökkääjän mahdollisuus muokata viestiä.

Alustusvektorien jaksotustarkkuus tarkoittaa periaatteessa sitä, että alustusvektori toimittaa paketin järjestysnumeron ja jos saapuvan paketin järjestysnumero on pienempi tai yhtä suuri kuin edellisen sanoman, niin se hylätään. Laskurit nollataan aina, kun asema neuvottelee uuden sessioavaimen. Tällä tekniikalla estetään tehokkaasti toistohyökkäykset.

Pakettikohtaisessa avainten sekoituksessa korjataan WEP-suojauksessa esille tullut RC4-algoritmin väärinkäyttö, TKIP-tekniikassa alustusvektori ja salausavain muuttuvat viestikohtaisesti. Sekoituksen ensimmäisessä vaiheessa langattoman laitteen MAC-osoite, salausavain ja viestilaskuri sekoitetaan pakettikohtaiseksi avaimeksi ja alustusvektoriksi. Väliaikainen avain vaihtuu 2^{16} paketin välein. Seuraavaksi väliaikainen avain sekoitetaan algoritmilla salaiseen avaimeen ja viestilaskuriin, josta saadaan 104–bittinen väliaikainen salausavain ja 24-bittinen alustusvektori.

Uudelleenavainnusmenetelmässä TKIP luo uuden tuoreen pakettikohtaisen avaimen, jota ei ole käytetty muiden asemien tai päätelaitteiden kanssa ja tieto avainten vaihdosta suoritetaan salatusti käyttämällä uudelleenavainnusavainta. [20.]

WLAN-yhteyttä muodostaessa tukiasema ja päätelaite suorittavat nelisuuntaisen kättelyn (four-way handshake), jossa ne muodostavat tarvittavat salausavaimet. Kuvassa 11 nähdään kättely. Se käydään tarkemmin läpi seuraavassa osiossa.



Kuva 11: WPA-PSK TKIP yhdistäminen

Molemmat sekä tukiasema että päätelaite tietävät yhteisen salasanansa, PSK:n. Tämän salasanan perusteella kumpikin muokkaa oman näennäissatunnaisen bittijononsa (Nonce). AP muodostaa Anoncen ja lähettää sen sekä MAC-osoitteensa STA:lle (1.), joka puolestaan muokkaa sen, MAC-osoitteiden, salausavaimen ja oman SNoncensa avulla väliaikaisen salausavaimen, PTK:n. Päätelaite lähettää AP:lle SNoncensa, MAC-osoitteensa ja MIC-tarkisteen (2.), joka on laskettu käyttäen avainvarmennusavainta. AP laskee taas vuorostaan saman PTK:n yhdistämällä MAC-osoitteet, salausavaimen sekä ANoncen ja SNoncen. Näin molemmat osapuolet saavat laskettua PTK:n ilman, että sitä pitää lähettää suojaamattomasti verkon yli. AP tarkistaa vielä viestin yhtenäisyyden eli MIC:n. Tämän jälkeen AP lähettää vielä MIC:n sekä väliaikaisen ryhmäavaimen (GTK), jonka se suojaa PTK:lla, jokaiselle päätelaitteelle (3.). Päätelaite lopettaa kättelyn lähettämällä MIC:n (4.) vielä kertaalleen, jonka jälkeen molemmat tallentavat väliaikaiset salausavaimet ja sanoma voidaan lähettää salatusti. [21.]

WPA-PSK TKIP -suojauksen heikkoutena on niin kutsuttu sanakirjahyökkäys. Käyttäjän valitessa salausavaimeksi jonkin yleisen selkokielisen sanakirjasta löytyvän sanan, sanakirjahyökkäys purkaa nauhoitetun liikenteen käyttämällä sanakirjassa esiintyviä sanoja ja saa selville käytössä olevan salausavaimen. Tällöin koko verkko on auki hyökkääjälle. Tapaa kutsutaa nimellä ”brute force attack” eli suojaus puretaan käyttämällä raakaa voimaa.

Toisena ongelmana voidaan nähdä tahallinen MIC-palvelunestohyökkäys, jolloin tukiasemalle lähetetään tarpeeksi monta väärää pakettia. Tällöin tukiasema katkaisee yhteyden kaikkiin yhteydessä oleviin laitteisiin. [21;22.]

6.5 IEEE 802.1X/EAP

802.1X-protokolla standardi antaa mahdollisuuden suojata langaton verkko käyttämällä autentikoivaa palvelinta ja käyttäjän tunnistusprotokollaa, tässä kappaleessa EAP (Extensible Authentication Protocol). 802.1X perustuu porttikohtaiseen verkkoyhteyden hallintaan (Port-Based Network Access Control), mikä tarkoittaa että ilman käyttäjän autentikointia ei verkkoyhteyteen pääse. EAP tarjoaa yhteisen mekanismin tukemaan useita eri autentikointitapoja niin langallisille kuin langattomillekin yhteyksille. Tässä insinöörityössä käydään läpi vain EAP-TLS ja EAP-TTLS.

6.5.1 EAP-TLS

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) on IETF:n (Internet Engineering Task Force) standardi, joka käyttää viimeisintä versiota SSL (Secure Socket Layer) -protokollasta, TLS-protokollaa. TLS:n avulla voidaan molemmat, sekä käyttäjä että palvelin varmentaa digitaalisten sertifikaattien avulla. Protokolla mahdollistaa myös vaihtuvien istuntokohtaisten avainten luomisen. [23.]

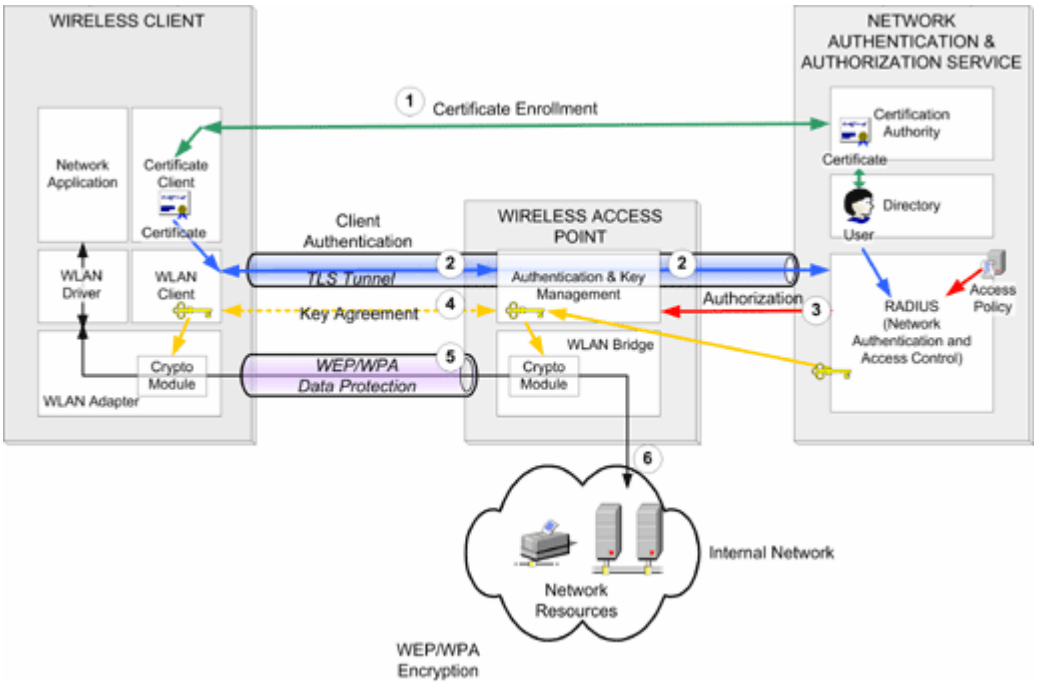
Kun aiemmissa suojaustavoissa on ollut käytössä vain päätelaite ja tukiasema, niin 802.1X/EAP:ta käytettäessä otetaan käyttöön kolmas elementti, varmentava palvelin. Tämä on AAA (Authentication, Authorization ja Accounting) -palvelin. Yleensä käytetään RADIUS (Remote Authentication Dial-In User Service) -palvelinta. Yleisesti käytössä olevat termit ovat päätelaitteelle asiakas (supplicant), tukiasemalle autentikaattori ja palvelimelle AS (Authenticating Server). [23.]

Sekä asiakas- että palvelinpään täytyy tukea EAP-TLS autentikointia, välissä oleva autentikaattori eli AP ole tietoinen EAP-protokollan tyypistä, joten sen täytyy tukea vain 802.1X/EAP-autentikointiprosessia. Jotta yhteyden muodostaminen onnistuu tarvii käyttäjälle ja palvelimelle määrittää sertifikaatit. Näin molemmat voivat varmistaa, että kyseessä on luotettava taho. Sertifikaattien purkamiseen käytetään PKI (Public Key Infrastucture) -konseptia, jossa EAP-TLS käyttää molemminpuolista TLS-autentikointia, jossa sekä

asiakas että palvelin todistavat ”henkilöllisyytensä” toisilleen sertifikaattien avulla. Autentikoinnissa käytetään kahta pääelementtiä; yksityis-julkinen avainpari ja sertifikointi auktoriteetti. [23.]

Jokaiseen sertifikaattiin on sidottu kaksi avainta, julkinen ja yksityinen, joista yksityisen tietää vain sertifikaatin omistaja ja julkisen avaimen kaikki. Tällä tavoin yksityisellä avaimella salattu sanoma voidaan purkaa vain julkisella avaimella ja sama toisinpäin. Luottamuksen toinen elementti on ulkopuolinen sertifikaatin myöntäjä (root certification authority), se voi olla joko julkinen tai yksityinen. Tällä tavoin voidaan varmistaa luoteltulta sertifikaatin allekirjoittajalta että vastapää on todellakin luotettava. Osa sertifikaatin sisällöstä on suojattu sertifikaatin myöntäjän julkisella avaimella ja siinä selviää kenelle se on myönnetty ja sertifikaatin voimassaoloaika. Jotta kirjautuminen onnistuisi, molemmilla pitää olla saman sertifikaatin myöntäjän sertifikaatti. Lisäksi asiakaskoneella täytyy olla sama käyttäjätunnus kuin palvelimen sertifikaatissa ja tunnuksen täytyy löytyä palvelimen tietokannasta. [23.]

Autentikoinnin lopuksi palvelin laskee istuntokohtaisen avaimen ja lähettää sen TLS putkessa autentikaattorille, samalla asiakaskone laskee saman avaimen ja autentikointi on valmis. Asiakas ja palvelinpään konfiguroinnista lisää lähteestä [23]. Kuva 12 antaa käsityksen EAP-TLS -autentikoinnista.



Kuva 12. EAP-TLS -autentikointi

6.5.2 EAP-TTLS

EAP-TTLS (Tunneling Transport Layer Security) kehitettiin laajentamaan edellisessä kappaleessa mainittua EAP-TLS-metodia. Vastoin EAP-TLS:n kättelyä, EAP-TTLS voi valita käyttääkö se vain yhdensuuntaista autentikointia, jossa palvelin varmistaa itsensä asiakkaalle vai käytetäänkö molemminpuolista kättelyä. EAP-TTLS välittää TLS kättelyn aikana lisätietoja asiakaskoneen ja palvelimen välillä, näiden tietojen avulla asiakaskone voi käyttää autentikointiin muitakin kuin EAP metodeja, esimerkiksi PAP-, CHAP-, MS-CHAP- ja MS-CHAPV2 -protokollia. EAP-TTLS voi myös käyttää erillistä AAA-palvelinta TLS-sessiolle ja toista palvelinta, niin kutsuttua koti-AAA-palvelinta autentikointiin, jolloin jälkimmäisen ei tarvi tukea EAP-TTLS-protokollaa. [24.]

6.6 IEEE 802.11i

IEEE 802.11i -lisäys 802.11-standardiin julkaistiin 24.6.2004, sitä kutsutaan myös WPA2:ksi. Lisäyksessä esitteltiin uusi tapa suojata liikenne käyttäen 128-bittistä AES (Advanced Encryption Standard) -algoritmia. AES käyttää salaukseen joko TKIP- tai CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) -protokollaa, TKIP on jätetty vanhemman WLAN-laitteiston yhteensopivuutta varten. IEEE 802.11i -standardin mukaisia turvallisuusratkaisuita käyttäviä langattomia lähiverkkoja kutsutaan RSN -verkoiksi (Robust Security Network).

AES-CCMP perustuu pitkälti käyttäjän autentikoinnissa aiemmin läpi käytyihin tekniikoihin. Se käyttää EAP-protokollaa käyttäjän autentikoinnissa RADIUS-palvelimen kanssa. Avainten muodostaminen tapahtuu nelisuuntaisessa kättelyssä, molemmat laskevat parikohtaisen väliaikaisen avaimen kättelyssä välitettyjen tietojen perusteella.

Counter Mode on lohkosalausmenetelmä joka salaa datan 128-bitin lohkoissa 128-bitin salausavaimella. Cipher Block Chaining Message Authentication Code, CBC-MAC -algoritmi muodostaa MIC:n joka varmentaa tiedon alkuperän ja oikeellisuuden. MIC ja data salataan sitten käyttämällä counter modea. Jokaisella salattavalla paketilla on yksilöllinen pakettinumero, jota käytetään pakettien toiston huomaamiseen. [25.]

6.7 VPN

Virtual Private Network, VPN, tarkoittaa vapaasti suomennettuna näennäistä yksityistä verkkoa. Se on tapa, jolla kaksi tai useampia yrityksen verkkoja, tai erillisiä etätyöpisteitä, voidaan yhdistää julkisen verkon yli. Yhteys verkkojen välillä tunneloidaan. Kaikki liikenne VPN:ssä salataan jonkin liikenteen salaavan protokollan sisään. Yleisesti käytössä olevia VPN-protokollia ovat IPSec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point to Point Tunneling Protocol). VPN perustuu myös vahvalle käyttäjän tunnistamiselle.

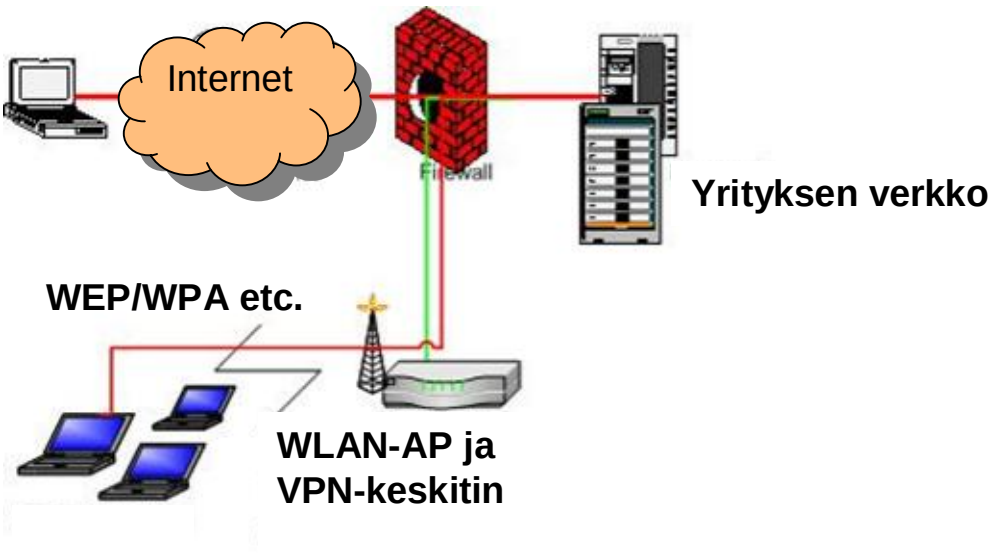
Langattomassa yhteydessä yritysverkon sisällä voidaan yhdistää VPN ja perinteiset suojausmetodit. STA:n ja AP:n välillä oleva yhteys voidaan jättää suojaamatta tai suojata esimerkiksi WEP/WPA-suojauksella. AP:lta eteenpäin yrityksen sisäverkkoon käytettäisiin VPN-yhteyttä. Tällä tavoin kuka tahansa saa yhteyden AP:lle, mutta AP:n jälkeen on vastassa VPN-keskitin, johon yhteys ilman vaadittavia tunnistaumistietoja pysähtyy.

Tässä työssä käydään läpi vain IPSec-protokollavaihtoehdot. Pakettivirtojen turvaamiseen IPSec tarjoaa kaksi vaihtoehtoista protokollaa, joista yleisimmin käytetty on ESP (Encapsulating Security Payload). Se salaa koko IP-paketin ja mahdollistaa samalla autentikoinnin. Toinen vaihtoehto on AH (Authenticating Headers), joka tarjoaa vain todennuksen ja takaa viestin eheyden, mutta ei tarjoa luottamuksellisuutta eli salausta. AH:n vajavuutena mainittakoon, ettei se tue osoitteenmuutosta (NAT).

IPSec:iä voidaan käyttään kahdella tavalla: kuljetus (transport) ja tunneli (tunnel). Kuljetuksessa luodaan suojattu yhteys kahden pisteen välille kapsuloimalla IP-paketin dataosio. Tunneloinnissa koko IP-paketti kapsuloidaan kuljetusprotokollan sisään, jolloin luodaan virtuaalinen yhteys lähettäjältä vastaanottajalle.

Kun IPSec-paketti saapuu VPN-keskittimelle tarvitaan jonkinlainen tunnistautumiskeino. Tämä on toteutettu suojausassosiaatiolla, SA (Security Association), jossa tarkistetaan saapuvasta paketista IP-osoite, IPSec-protokolla ja suojaustapa. Näitä tietoja verrataan tietokantaan, SADB (Security Associations Database). IPSec käyttää autentikoinnissa joko manuaalisesti määritettyjä avaimia tai IKE:ä (Internet Key Exchange), jossa avaimet muodostetaan verkon yli. Yleensä käytössä on manuaalinen avainten määrittely. Tä-

mä toimii esimerkiksi yrityksen WLAN-yhteyksissä samoilla tunnuksilla kuin normaaliin LAN-verkkoon kirjautuminen työkoneella. Yksi tunnistautumisvaihtoehto on sirukortti. Se luo ainutlaatuisen ja vain sillä kertaa voimassa olevan, vaihtuvan pääsykoodin. Pääsykoodia on mahdollista käyttää yhdessä salaisen, henkilökohtaisen pin-koodin tunnistuksen varmentamiseksi. Älykorttien avulla käyttäjien tunnistus on helppoa ja kortin mukana kuljettaminen on vaivatonta käyttäjälle. [26.]



Kuva 13. VPN-yhteyden elementit

7 JOHTOPÄÄTÖKSET

Langattoman lähiverkon suunnittelemisessa kannattaa ottaa ensimmäisenä huomioon verkon käyttäjien määrä ja käyttötarve, onko kyseessä vierailijoille tarjottava verkko vai tuleeko siitä päästä myös esimerkiksi tiedostopalvelimelle. Yleensä kotikäyttäjillä on tarpeena saada langaton verkko kotikoneiden välille, kun taas yrityksillä tarpeena on pääsy palvelimelle ja arkaluontoisiin tietoihin.

Kotikäyttäjille tarjotaan Suomessa tällä hetkellä laajakaistaliittymien kylkiäisinä kannettavia tietokoneita ja WLAN-modeemeita. Tämä on aiheuttanut räjähdysmäisen kasvun langattomien yhteyksien käytössä. Moni käyttäjä kytkee modeemin seinään, asentaa virustorjuntaohjelmiston koneellensa ja käyttää WLAN-yhteyttä suojaamattomasti, tästä seuraa yhteyden luvaton käyttö. Suomessa on jo yksi rikostapaus, jossa jaettua naapurin yhteyttä käytettiin rikosten tekemiseen. Tämän takia on tärkeä suojata yhteys ja salata liikenne.

Kotiverkko

Kotikäyttäjän tulisi ennen WLAN-tukiaseman käyttöönottoa suojata yhteys. WEP-suojaus estää tahattomat yhteydenotot ja saattaa hidastaa tahallista murtautujaa, mutta ajan kanssa yhteys on varmasti murrettu ja pahimmassa tapauksessa murtautuja saa asiakkaan koneen haltuunsa. Tämän vuoksi on suositeltavaa valita suojaustavaksi WPA-PSK TKIP. Tämäkin suojaus on kuitenkin lähes hyödytön hakkereita vastaan, jos käyttäjä käyttää salausavaimena sanakirjasta suoraan löytyvää sanaa, kuten computer. Käyttämällä tarpeeksi pitkää salasanaa ja lisäämällä siihen numeroita ja muita merkkejä, voidaan murtautuminen tehdä lähes mahdottomaksi. WPA:n lisäksi voidaan käyttää MAC-suodatusta ja SSID:n piilotusta varotoimenpiteenä. MAC-suodatusta kannattaa käyttää harkiten, jos verkossa koneiden vaihtuvuus on suuri. Jatkuva listojen ylläpitäminen saattaa käydä rasittavaksi.

Nykyään on suurimmassa osassa WLAN-tukiasemista myös ohjelmallinen palomuuri ja NAT-osoitteenmuutos. Nämä ominaisuudet kannattaa tarkistaa ostovaiheessa, sillä lisäturva virusten aiheuttamille hyökkäyksille ei ole koskaan pahitteeksi. Kannattaa ottaa huomioon myös se, että laitevalmistajat

julkaisevat ohjelmistopäivityksiä laitteille. Koska suojaustapojen kehittely on jatkuvaa, saattaa parempi suojaustapa olla päivityksen jälkeen saatavissa.

Yritysverkko

Yritysten sisäisissä WLAN-yhteyksissä kannattaa ottaa huomioon miten yhteydet jaetaan. Erilliset WLAN-yhteydet vierailijoille ja yrityksen sisäverkkoon yhteyttä tarvitseville omat. Kuten aiemmissa kappaleissa on käyty läpi, kannattaa yrityksen verkkoon pyrkijät varmentaa autentikoivalta palvelimelta. Yritysten tukiasemien sijoittelu kannattaa myöskin suunnitella tarkoin, päällekkäisten kanavien häirintä tuli ottaa huomioon.

Eräs tärkeä asia on myös työntekijöiden kannettavien tuki suojauksille, vanhemmat sovittimet eivät välttämättä tue kaikkia suojaustapoja. Laitteiston ohjelmistopäivitykset tulisi pitää ajan tasalla ja laitteiston uusiminen mielessä. Vain 802.11b:tä tukevat laitteet tulisi ainakin uusia, sillä ne hidastavat uudempien 802.11g käyttäjien verkkoyhteyttä.

Laite- ja ohjelmistovalmistajien vahva tuki turvallisille ja helposti hallittaville langattomille tekniikoille madaltaa organisaatioiden kynnystä hyödyntää niitä. CCMP-tekniikkaa hyödyntävä verkko on nykytiedon mukaan turvallinen, sillä AES-algoritmia, sen CCM-sovellutusta, tai IEEE 802.11i-avaintenhallintamekanismia vastaan ei tunneta käytännöllisiä tai tehokkaita hyökkäyksiä, joilla voidaan vaikuttaa viestinnän eheyttä tai luottamuksellisuutta heikentävästi.

Avoimessa WLAN-verkossa otettava VPN-yhteys saattaisi olla paras ratkaisu. Käyttäjän ei tarvitse varmentaa itseään tukiasemalle, vain VPN-yhteyden muodostus vaatisi autentikoinnin. Tällä tavoin voitaisiin säästää laitekuluissa, koska mitään suojausta ei tarvisisi tukea. Tukiasema tulisi tällöin määritellä päästämään läpi vain VPN-yhteyteen tarvittava liikenne (IPSec, L2TP, PPTP).

Teknisen haavoittuvuuden löytymistä suurempana riskinä langattomien verkojen turvallisuudelle onkin ehkä inhimillinen, kuten verkkosalasanan tai varmenteiden vuotaminen ulkopuolisille vahingossa. Jos verkon koko on muutamaa asemaa suurempi, on keskitetyn todennuspalvelun käyttäminen edellytys IEEE 802.11-verkkojen turvalliseen hyödyntämiseen.

VIITELUETTELO

[1] Puska, J (2005). Langattomat lähiverkot. Talentum Media Oy.

[2] Geier, Jim (2005). Langattomat verkot – perusteet. IT Press.

[3] Nicopolitidis, P. - Obaidat, M. S. - Papadimitrou, G. I. – Pomportsis, A. S. (2003). Wireless Networks. John Wiley & Sons.

[4] Prasand, Neeli ja Anand (2002). WLAN Systems and Wireless IP for Next Generation Communications. Artech House Books.

[5] Santamariá, Asunción - López-Hernández, Francisco J. (2001). Wireless LAN – Standards and Applications. Artech House Books.

[6] Granlund, Kaj (2001). Langaton tiedonsiirto. Docendo Finland Oy.

[7] Dodd, Annabel Z. (2005). The Essential Guide to Telecommunications (4. painos). Prentice Hall PTR.

[8] Vacca, John R. (2002). Wireless data demystified. McGraw-Hill.

[9] Webb, William (2001). The Future of Wireless Communications. Artech House Books.

[10] Geier, Jim (31.7.2002). 802.11a: An Excellent Long Term Solution. [Verkko-dokumentti, viitattu 23.3.2007]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/10724_1436331_1.

[11] IEEE Standards Association. (päivitetty 12.6.2003). 802.11a-1999: Part 11: Wireless LAN Medium Access (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band. [Verkkojulkaisu, viitattu 23.3.2007]. Saatavissa: http://standards.ieee.org/getieee802/download/802.11a-1999.pdf.

[12] IEEE Standards Association. (27.7.2003). 802.11g: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. [Verkkojulkaisu, viitattu 23.3.2007]. Saatavissa: http://standards.ieee.org/getieee802/download/802.11g-2003.pdf.

[13] IEEE Standards Association. IEEE 802.16 Published Standards and Drafts. [Verkkojulkaisu, viitattu 26.3.2007]. Saatavissa: http://www.ieee802.org/16/published.html.

[14] Viestintävirasto (8/2005). Langattomat Laajakaistaratkaisut [Verkkodokumentti, viitattu 26.3.2007]. Saatavissa: http://www.ficora.fi/attachments/suomi_R_Y/1158858938123/Files/CurrentFile/TRaportti082005.pdf.

[15] IEEE Standards Association (19.9.2006). IEEE-SA adopts plan to move 802.20™ Broadband Wireless Standard forward. [Verkkojulkaisu, viitattu 26.3.2007]. Saatavissa: http://standards.ieee.org/announcements/pr_80220plan.html.

[16] IEEE Standards Association (6.12.2006). Extension Approval of Project - 802.20 [Verkkodokumentti, viitattu 26.3.2007]. Saatavissa: http://standards.ieee.org/board/nes/projects/802-20.pdf.

[17] Geier, Eric (10.1.2006). Your SSID Isn't Hidden Forever. [Verkkojulkaisu, viitattu 27.3.2007]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/3576541.

[18] Borisov, Nikita - Goldberg, Ian - Wagner, David (2001) Intercepting Mobile Communications: The Insecurity of 802.11. [Verkkodokumentti, viitattu 28.3.2007]. Saatavissa: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[19] Cheung, Humphrey (31.3.2005). The Feds can own your WLAN too. [Verkkojulkaisu, viitattu 28.3.2007]. Saatavissa: http://www.smallnetbuilder.com/content/view/24251/100/.

[20] Walker, Jesse (26.7.2003). 802.11 Security Series, Part II: The Temporal Key Integrity Protocol (TKIP) [Verkkodokumentti, viitattu 29.3.2007]. Saatavissa: http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf.

[21] Phifer, Lisa (23.3.2007). WPA PSK Crackers: Loose Lips Sink Ships. [Verkkojulkaisu, viitattu 30.3.2007]. Saatavissa: http://www.wi-fiplanet.com/tutorials/article.php/10724_3667586_1.

[22] Peikari, Cyrus – Fogie, Seth (30.12.2004). WPA Part 3: WPA Fixes. [Verkkojulkaisu, viitattu 29.3.2007]. Saatavissa: http://www.informit.com/guides/content.asp?g=security&seqNum=86&rl=1.

[23] Cisco Systems, Inc. EAP-TLS Deployment Guide for Wireless LAN Networks. [Verkkojulkaisu, viitattu 30.3.2007]. Saatavissa: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml.

[24] Cisco Systems, Inc (10.3.2006). Extensible Authentication Protocols. [Verkkojulkaisu, viitattu 5.4.2007]. Saatavissa: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/4_1/users/eap.pdf.

[25] Microsoft Corporation (1.11.2006). Wi-Fi Protected Access 2 (WPA2) Overview. [Verkkojulkaisu, viitattu 5.4.2007]. Saatavissa: http://www.microsoft.com/technet/community/columns/cableguy/cg0505.mspx.

[26] Friedl, Steve (24.8.2005). An Illustrated Guide to IPsec. [Verkkojulkaisu, viitattu 8.4.2007]. Saatavissa: http://www.unixwiz.net/techtips/iguide-ipsec.html.